УДК 004.732.056

РОЗРОБКА СИСТЕМИ ІДЕНТИФІКАЦІЇ ШКІДЛИВОГО ПРОГРАМНОГО ЗАБЕЗПЕЧЕННЯ НА ОСНОВІ КОНТЕКСТНО-ВІЛЬНИХ ГРАМАТИК

***В.В. ЧЕЛАК*[1*], *С.Ю. ГАВРИЛЕНКО*[2**]**

[1] *магістрант кафедри «Обчислювальна техніка та програмування», НТУ «ХПІ», Харків, УКРАЇНА*

[2] *професор кафедри «Обчислювальна техніка та програмування», канд. техн. наук, НТУ «ХПІ», Харків, УКРАЇНА*

[*] *email: victor.chelak@gmail.com*

[**] *email: Gavrilenko08@gmail.com*

У сучасному суспільстві для задоволення його потреб виникають проблеми інформаційного забезпечення всіх сфер діяльності людини. Одна з таких проблем – забезпечення надійного захисту інформації. Особливої гостроти вона набуває у зв'язку з масовою комп'ютеризацією усіх сфер діяльності суспільства.

Одну з найзначніших загроз безпеці комп'ютерних систем та інформації в цілому складає шкідливе програмне забезпечення, або комп'ютерні віруси. Обсяги комп'ютерних вірусів та шкідливого програмного забезпечення щорічно збільшуються [1]. В даний час не існує такої антивірусної програми, яка могла б виявити всі вірусні загрози [2-5].

В доповіді запропоновано модель аналізу шкідливого програмного забезпечення на основі контекстно-вільних граматик.

Проаналізовано шкідливе програмне забезпечення сімейств Trojan, Worm, Adware, виділено характерні ознаки. Розглянуто механізм роботи кріптолокерів типу Petya. Вірус NotPetya шифрує файли з певними розширеннями, а також перезаписує MBR (Master Boot Record), очищає лог-файли (журнали подій), виконує перезавантаження комп'ютера та виводить повідомлення з вимогою викупу.

Зразок отримує аутентифікаційні дані за допомогою функції CredEnumerate і утиліти mimikatz. За допомогою отриманих даних виконується поширення мережею за рахунок підключень до ресурсу admin$, утиліти PsExec.exe і wmic.exe (WMI). Також виконуються спроби експлуатації вразливостей SMB EternalBlue (CVE-2017-0144) і EternalRomance (CVE-2017-0145).

За результатами аналізів, виділено перелік дій вірусу NotPetya, які у сукупності є шкідливими, а саме:

- Перевірка послідовностей на наявність хеш-сум назв антивірусного ПО.
- Звертання до великої кількості різнотипних файлів.
- Використання алгоритму шифрування за допомогою відкритого ключа.
- Використання утиліти mimikatz для вилучення облікових даних.

– Спроби отримати права адміністратора, підключення до різних ресурсів.
– Використання функцій отримання інформації про ресурси мережі.
– Спроба використання вразливостей SMB-механізму.
– Спроба отримати права адміністратора.
– Спроба перезапису MBR.
– Перезавантаження комп'ютера.

Розроблено систему ідентифікації шкідливого програмного забезпечення (ПЗ) що базується на множині магазинних автоматів та визначається наступною сукупністю семи об'єктів:

$$M=\{P, S, s_o, f, F, H, h_o\}, \quad (1)$$

де P – вхідний алфавіт, S – алфавіт станів, s_o – початковий стан, $s_o \in S$, F – множина кінцевих станів , H – алфавіт магазинних символів, h_o – маркер дна магазину, $h_o \in H$, f – функція переходів.

Кожний із магазинних автоматів задається правилами граматики, які зберігаються у файлах (рис.3-5). У якості граматики використано LL(1) граматику, для яких детермінований розпізнавач працює по одному вхідному символу, розташованому в поточній позиції.

Розроблене ПЗ генерує команди для кожного магазинного автомату та перевіряє вхідний файл на наявність вибраних ознак для заданого класу шкідливого програмного забезпечення. Завдання порогової кількості вибраних ознак дозволяє зробити висновок про враження комп'ютерної системи. Виконано тестування розробленої системи.

Проведені експериментальні дослідження підтверджують можливість використання запропонованого підходу, як додаткового засобу для виявлення вірусних атак, в загальній системі виявлення шкідливого програмного забезпечення.

Список літератури:

1. *Унечек Р.* Развитие информационных угроз в первом квартале 2017 года. Статистика. [Електронний ресурс] / *Р. Унечек, Ф. Синицын, Д. Паринов, В. Столяров* // Режим доступу: https://securelist.ru/analysis/malware-quarterly/30657/it-threat-evolution-q1-2017-statistics/

2. *Шелухин О.И.* Обнаружение вторжений в компьютерные сети / *О.И. Шелухин, Д. Ж Сакалема, А.С. Филинова.* – М.: Гарячая линия-Телеком, 2013. – 220 с.

3. *Гошко С.В.* Технологии борьбы с компьютерными вирусами / *С.В. Гошко*. – М.: Солон-Пресс, 2009. – 352 с.

4. *Касперски К.* Записки исследователя компьютерных вирусов / *К. Касперски*. – СПб.: Питер, 2012. – 316 с.

5. *Касперски К.* Компьютерные вирусы изнутри и снаружи / *К. Касперски*. – СПб.: Питер, 2011. – 527 с.

6. *Климентьев К.Е.* Компьютерные вирусы и антивирусы: взгляд программиста / *К.Е. Климентьев.* – М.: ДМК, 2013. – 185 с.